The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
06/14/2011

SUBJECT:
Vulnerability in OLE Automation Could Allow Remote Code Execution (MS11-038)

OVERVIEW:
A remote code execution vulnerability has been discovered in Microsoft Windows Object Linking and Embedding (OLE) Automation. OLE Automation is a Windows protocol that provides a platform for applications to access and manipulate functionalities that are made available by other applications. This vulnerability can be exploited if a user views a specially crafted Windows Metafile (WMF) image on a web page or by opening a specially crafted WMF file as an email attachment.

Successful exploitation will result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, the attacker could then install programs; view, change, or delete data; or create new accounts with full privileges.

SYSTEMS AFFECTED:

- Windows XP
- Windows 7
- Windows Server 2003
- Windows Vista
- Windows Server 2008

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
A remote code execution vulnerability has been discovered in Microsoft Windows Object Linking and Embedding (OLE) Automation. This vulnerability exists due to the way Windows OLE Automation parses specially crafted WMF files. This vulnerability can be exploited if a user views a specially crafted Windows Metafile (WMF)image on a web page or by opening a specially crafted WMF file as an email attachment.

Successful exploitation will result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, the attacker could then install programs; view, change, or delete data; or create new accounts with full privileges.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Do not visit untrusted websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.
- Consider implementing file extension whitelists for allowed e-mail attachments.

REFERENCES:
Microsoft:
http://www.microsoft.com/technet/security/bulletin/ms11-038.mspx

Sophos:
http://www.sophos.com/support/knowledgebase/article/113723.html

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0658

Security Focus:
http://www.securityfocus.com/bid/48174